UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/524,854	02/18/2005	Francois Sendra	09669/053001	8308

22511 7590 12/03/2008

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
MACILWINEN, JOHN MOORE JAIN	
ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
12/03/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/524,854	SENDRA, FRANCOIS	
	Examiner	Art Unit	
	John M. MacIlwinen	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7/18/2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see pgs. 9 - 20, filed 7/18/2008, with respect to the rejection(s) of claim(s) 19-36, have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Gong et al. (Going Beyond the Sandbox: An Overview of the New Security Architecture in Java Development Kit 1.2), Sun's Java Plug-in Technology (http://web.archive.org/web/20040209165208/http://java.sun.com/products/plugin/), and Gasparini (US 2004/0168083 A1).

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 19 - 29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

4. Said claims are directed to "a data processing device" or a "data processing system"; however, said device/system is described solely as comprising a "browser" and "a plug-in"; i.e., software.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 19, 24, 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gong (Going Beyond the Sandbox: An Overview of the New Security Architecture in Java Development Kit 1.2) and Sun's Java Plug-in Technology (http://web.archive.org/web/20040209165208/http://java.sun.com/products/plugin/), hereafter Sun.

7. Regarding claim 19, Gong shows a data processing device configured to communicate with a plurality of resources via a browser, comprising:

the browser (3.1) comprising a first private zone and a second private zone (represented by protection domains, 2.3), wherein the first private zone and the second private zone are each configured to be allocated to a respective set of resources of the plurality of resources to store information (2.1, paragraphs 2 - 3, where the protection domains (2.3) are allocated to code from websites, which represent the claimed 'respective set of resources'); and

ensuring that the respective set of resources communicate exclusively with the first private zone allocated to the respective set of resources (2.3, paragraphs 2-4).

Gong does not explicitly show where the exclusive communication is ensured by a plug-in, but does show where a browser (3.1, paragraph 1) can be used to implement Gong's security architecture, which includes the utilization of private zones (2.3).

Sun shows where the a Java JRE plug-in connects Java to a browser (page 1), which allows/enables the security architecture disclosed by Gong (Gong, 3.1

paragraphs 2 and 3).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong with that of Sun as the both Gong and Sun teach utilizing Java, and are designed to be used together (Gong, Section 3.1, Sun, pg. 1).

8. Regarding claim 24, Gong in view of Sun and further show a manager comprising code instructions adapted to manage the use of the data processing device (Gong, 3.1, paragraph 2), wherein the plug-in further comprises functionality to manage, upon request, allocation of a first private zone to the respective set of resources by supplying information to the respective set of resources, wherein information comprises a reference of the first private zone (Gong, 2.3, paragraphs 7 and 8).

9. Regarding claim 25, Gong in view of Sun further show a data processing device communicating with a computer resource via a network, wherein the data processing device comprises:

a browser (Gong, 3.1), and

a plug-in (Sun, pg. 1), which, when executed, is configured to obtain an allocation of a private zone, wherein the allocation ensures that the communication between the private zone and the computer resource is exclusive (Gong, 2.3).

10. Regarding claim 26, Gong in view of Sun further show wherein the private zone is managed by an entity, wherein the entity is configured to allocate the private zone to the computer resource (Gong, 2.3) and transmits security parameters to the computer resource, wherein the parameters identify the private zone (Gong, 2.4, paragraphs 6 – 7).

11. Claims 20, 21, 22, 23, 27, 28 30 – 33, 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gong in view of Sun as applied to claim 19 above, and further in view of Gasparini (US 2004/0168083 A1).

12. Regarding claim 20, Gong in view of Sun further show wherein the plug-in comprises at least one input parameter corresponding to a zone access key (Gong, 2.1, paragraph 2, where the plug-in enables the execution of the Java runtime, which allows capture and thus utilization of public/private keys and digital signatures), wherein the plug-in, after execution and depending on the zone access key, is able to authorize access to the first private zone and deny access to the second private zone of the browser (Gong, 2.1, 2.3, where the 'protection domains' represent the claimed 'private zone' and where, through the plural 'domains', shows at least a first and a second domain/zone).

Gong in view of Sun further show where public/private keys and digital signatures are used to match code from websites/URLs to their corresponding protection domains (2.1,2.3), but do not explicitly show wherein a value of the zone access key is supplied through a secured transmission by the respective set of resources corresponding to the first private zone.

Gasparini, like Gong in view of Sun, also shows utilizing public/private keys and digital signatures (Gasparini, [37]), and Gasparini also shows where a value of the zone access key is supplied through a secured transmission ([26]) by the respective set of resources ([37, 40 – 44]).

It would have been obvious to one of ordinary skill in the art to modify the

teachings of Gong in view of Sun with that of Gasparini in order to elaborate on the teachings in Gong in view of Sun of using public/private keys with the more specific disclosure in Gasparini for using keys and digital signatures for authentication and verification (such as for verifying access rights for both the data processing device comprising the browser and the respective set of resources).

Gong in view of Sun and Gasparini thus disclose all of claim 20.

13. Regarding claim 21, Gong in view of Sun and Gasparini further show wherein the respective set of resources performs authentication by transmitting a request to the browser prompting the user to enter the zone access key received (Gasparini, [27-30, 36, 40] and Fig. 3A) and if the access key is correct, the plug-in (Sun, pg. 1 and Gong, 3.1) comprises code instructions adapted to manage authentication between a respective set of resources and a corresponding allocated private zone from a group consisting of the first private zone and the second private zone (Gong, 2.1 paragraphs 2 and 3, 2.3, paragraphs 2 and 3).

14. Regarding claim 22, Gong in view of Sun and Gasparini further show wherein the first private zone and the second private zone are each configured to store information (Gong, section 2.3, paragraph 2, and Sun, pg. 1) wherein information comprises security information ensuring securing communication between at least one of a group consisting of the first private zone and the second private zone, and the respective set of resources (Gong, 2.1, 2.3).

15. Regarding claim 23, Gong in view of Sun and Gasparini further show wherein the data processing device interprets code (Sun, pg. 1, Gong, 3.1) instructions which, after

authentication and using security information (Gong, 2.1, Gasparini, [37]) stored in at least one of the first private zone and the second private zone (Gong, 2.3, paragraph 2, 2.6 paragraph 1), is configured to manage the administration of the at least one of the first private zone and the second private zone as well as use of application data (Gong, 2.4, paragraphs 1 – 2, 3.3) in at least one of the first private zone and the second private zone during a communication between the browser and the respective set of resources (Gong, 2.3, 3.4).

16. Regarding claim 27, Gong in view of Sun show claim 26, including where encrypted information is stored in the private zone (Gong, 2.1, paragraphs 3 – 7)

Gong in view of Sun do not explicitly show all of where the entity is further configured to transmit to the computer resource at least one master key previously stored in the private zone, and

the at least one master key is configured to encrypt information transmitted between the private zone and the computer resource.

Gasparini shows transmitting to the computer resource at least one master key previously stored in the private zone ([37, 40]), and

the at least one master key is configured to encrypt information transmitted between the private zone and the computer resource ([40, 55]).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong in view of Sun with that of Gasparini in order to elaborate on the teachings in Gong in view of Sun of using public/private keys with the more specific disclosure in Gasparini for using keys and digital signatures for authentication and

verification (such as for verifying access rights for both the data processing device comprising the browser and the respective set of resources).

17. Regarding claim 28, Gong in view of Sun and Gasparini further show a secured means configured to transmit a key to the data processing device to access the private zone, wherein the data processing device uses the key during communication to authenticate the private zone with the computer resource (Gasparini, [26, 37 – 40, 54-55]).

18. Regarding claim 30, Gong shows a method for communication using a data processing device, comprising creating in a browser, a first private zone and a second private zone (Gong, 2.3, 2.6, 3.1), wherein each of the first private zone and the second private zone is configurable to be allocated to a respective set of resources and store security information (2.1, 2.3, paragraph 2, 2.6)

allocating a first private zone to a respective set of resources (2.1) and

communicating between the allocated private zone and the respective set of resources, where access is denied during the communication to the second private zone (2.3, paragraphs 2-4).

Gong does not explicitly show where the exclusive communication is ensured by a plug-in, but does show where a browser (3.1, paragraph 1) can be used to implement Gong's security architecture, which includes the utilization of private zones (2.3).

Sun shows where the a Java JRE plug-in connects Java to a browser (page 1), which allows/enables the security architecture disclosed by Gong (Gong, 3.1 paragraphs 2 and 3).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong with that of Sun as the both Gong and Sun teach utilizing Java, and are designed to be used together (Gong, Section 3.1, Sun, pg. 1).

Gong in view of Sun do not explicitly show where the communication between the private zones and the respective set of resources are secured.

Gasparini shows securing information exchange between sites, including where the communication between the private zones and the respective set of resources is secured ([26, 37-40]).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong in view of Sun with that of Gasparini in order to elaborate on the teachings in Gong of using public/private keys with the more specific disclosure in Gasparini for using keys and digital signatures for authentication and verification (such as for verifying access rights for both the data processing device comprising the browser and the respective set of resources) as well as teachings in Gasparini of using SSL for encrypted communication.

19. Regarding claim 31, Gong in view of Sun and Gasparini further show wherein allocating the first private zone is managed by an entity, wherein the entity allocates the first private zone to the respective set of resources by supplying information comprising a reference of the first private zone (Gong, 2.3, 2.4, paragraphs 6 – 7).

20. Regarding claim 32, Gong in view of Sun and Gasparini further show wherein information supplied comprises a value of a master key stored in the first private zone, wherein the master key is able to encrypt information transmitted between the first

private zone and the respective set of resources (Gong, 2.1, Gasparini, [26,37-40, 55-56]).

21. Regarding claim 33, Gong in view of Sun and Gasparini further show wherein the respective set of resources transmits, by secured transmission means, an access key associated with the first private zone, wherein the access key is used to execute a plug-in, after execution, is able to ensure that the respective set of resources communicate exclusively with the first private zone (Gong, 2.3, 2.6, 3.1 and Gasparini, [37-44]).

22. Regarding claim 35, Gong in view of Sun and Gasparini further show wherein the data processing device is configured to communicate with a plurality of resources via a browser, wherein the browser comprises a plurality of private zone, wherein each private zone is configured to be allocated to a respective set of resources and store information specific to the respective set of resources (Gong, 2.3, 2.4 paragraphs 7 - 8),

wherein the plug-in (Sun, pg. 1) comprises at least one input parameter corresponding to a key to access at least one of the plurality of private zones (Gong, 2.1), wherein the value of the key is supplied to the data processing device by the respective set of resources (Gong, 2.1, Gasparini, [37-40]), and

wherein the plug-in, after execution, authorizes access to the at least one of the plurality of private zones according to the key (Gasparini, [37-40] and Gong, 2.1).

23. Regarding claim 36, Gong in view of Sun and Gasparini further show functionality to create, in a browser, a first private zone and a second private zone, wherein each of the first private zone and the second private zone is configurable to be allocated to a respective set of resources and store security information (Gong, 2.3, 2.4 paragraphs 7

- 8) ensuing secured communication between at least one of the first private zone and the second private zone and the respective set of resources (Gasparini, [26, 37-40, 55-56])

allocate the first private zone to the respective set of resources (Gong, 2.1) and

communicate between the allocated private zone and respective set of resources, wherein a plug-in denies access during the communication to the second private zone (Gong, 2.3).

24. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gong in view of Sun and Gasparini as applied to claim 30 above, and further in view of Sandhu et al. (US 6,985,953 B1).

25. Gong in view of Sun and Gasparini show claim 30, including where plug-ins can be transmitted to add additional functionality to browsers (Gong, 3.1, Sun, pg.1) as well as where security information is stored in private zones (Gong, 2.1, 2.3).

Gong in view of Sun and Gasparini do not explicitly show all of where in order to open a secured transaction, the respective set of resources transmits a plug-in, wherein the plug-in is configured to check whether security information written in at least one from the group consisting of the first and second private zones corresponds to the security information stored in memory attached to the respective set of resources.

Sandhu shows where in order to open a secured transaction, the respective set of resources transmits a plug-in, wherein the plug-in is configured to check whether security information written in at least one from the group consisting of the first and second private zones corresponds to the security information stored in memory

attached to the respective set of resources (col. 3 lines 7 – col. 4 line 19, col. 11 line 35 - col.12 line 24).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong in view of Sun and Gasparini with that of Sandhu in order to supply additional software to further ensure secure transmissions (Sandhu, col. 12 lines 10 - 24).

26. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gong in view of Gasparini.

27. Regarding claim 29, Gong shows a data processing system comprising a browser comprising a plurality of private zones (2.3, 2.6, paragraphs 1 and 2, 3.1),

a data processing device configured to communicate with a plurality of sites via the browser (2.6, paragraphs 1 and 2, 3.1),

wherein each of the plurality of private zones is configured to be allocated to the plurality of sites and store security information (2.3, paragraphs 2-3),

wherein the browser interprets code instructions stored on the data processing device ensuring that the plurality of sites communicates exclusively with an allocated private zone of the plurality of private zones (2.3, paragraphs 2-4).

Gong does not explicitly show where the communication between the data processing device and the plurality of sites is secured.

Gasparini shows securing information exchange between sites, including where the communication between the data processing device and the plurality of sites is secured ([26, 37-40]).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Gong with that of Gasparini in order to elaborate on the teachings in Gong of using public/private keys with the more specific disclosure in Gasparini for using keys and digital signatures for authentication and verification (such as for verifying access rights for both the data processing device comprising the browser and the respective set of resources) as well as teachings in Gasparini of using SSL for encrypted communication.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2442

John MacIlwinen

(571) 272 - 9686